BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 032 107**
A1

(12) # EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: 80810391.5

(22) Anmeldetag: 15.12.80

(51) Int. Cl.³: H 04 L 9/00

(30) Priorität: 20.12.79 CH 11319/79

(43) Veröffentlichungstag der Anmeldung: 15.07.81 Patentblatt 81/28

(84) Benannte Vertragsstaaten: CH DE FR GB LI NL SE

(71) Anmelder: GRETAG Aktiengesellschaft
Althardstrasse 70
CH-8105 Regensdorf(CH)

(72) Erfinder: Mueller, Kurt Hugo, Dr.
Höhenstrasse 15 A
CH-8304 Wallisellen(CH)

(74) Vertreter: Pirner, Wilhelm et al,
Patentabteilung der CIBA-GEIGY AG Postfach
CH-4002 Basel(CH)

(54) **Chiffrier/Dechiffriersystem.**

(57) Der Chiffrierteil (E) umfasst neben der eigentlichen Chiffriereinheit (1) einen Zufallsgenerator (3) und einen Grundschlüsselspeicher (2) sowie eine Auswahlstufe (4). Der Dechiffrierteil (D) umfasst eine Dechiffriereinheit (5), einen Grundschlüsselspeicher (6) und eine Verteilerstufe (7). Bei Beginn jeder Uebertragung und nach Störungen etc. werden Chiffrier- und Dechiffrierteil zunächst mittels einer Synchronisationssequenz synchronisiert. Dann wird durch den Zufallsgenerator eine Zufallsadresse für einen Grundschlüssel (PK) sowie ein zufälliger Zusatzschlüssel (AK) erzeugt. Adresse und Zusatzschlüssel werden dann klar übertragen und Grund- und Zusatzschlüssel in die Chiffrier bzw. Dechiffriereinheit geladen. Die zufallsgesteuerte, statistische Auswahl des Grundschlüssels vereinfacht das Schlüsselmanagement und damit die Bedienung des Systems.

EP 0 032 107 A1

./...

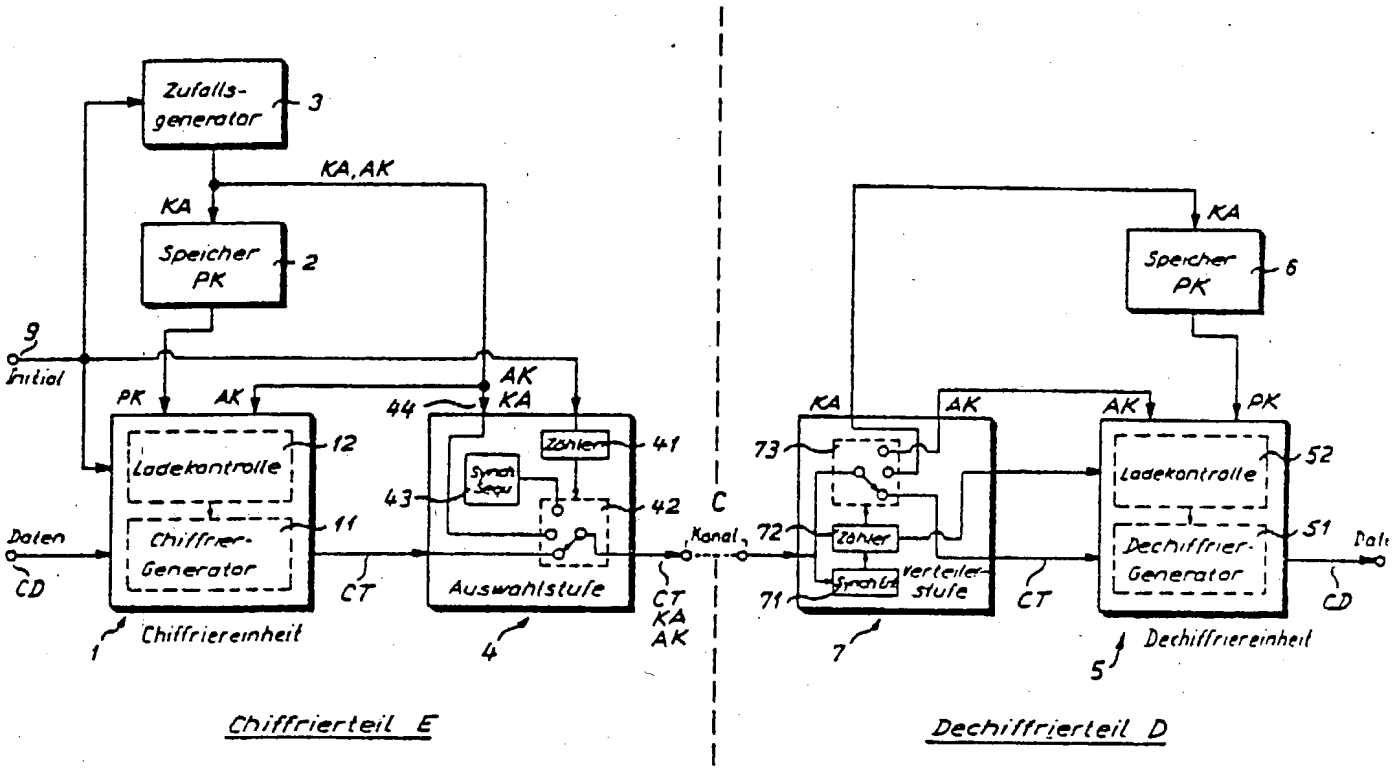

Zufalls-
generator
3
KA,AK
KA
Speicher
PK
2
9
Initial
PK
AK
AK
KA
44
Ladekontrolle
12
Chiffrier-
Generator
11
Daten
CD
CT
Zähler
41
Synch
Segu
43
42
Auswahlstufe
CT
KA
AK
1
Chiffriereinheit
4
C
Kanal
72
73
71
Zähler
Synch
Verteiler-
stufe
CT
7
KA
Speicher
PK
6
AK
PK
Ladekontrolle
52
Dechiffrier-
Generator
51
CD
5
Dechiffriereinheit
Chiffrierteil E
Dechiffrierteil D

Fig. 1

GRETAG AG,
Regensdorf (Schweiz)

7-12650/=

Chiffrier/Dechiffriersystem

Die Erfindung betrifft ein Chiffrier/Dechiffriersystem gemäss Oberbegriff des Patentanspruchs 1.

Typische Vertreter solcher Chiffrier/Dechiffriersysteme sind beispielsweise die Systeme GC-201 , GC-505 und GC-515 der Firme Gretag AG, Regensdorf, Schweiz. Diese Systeme enthalten als Kernstück einen Chiffrier/Dechiffriergenerator, dessen Struktur und Anfangszustände u.a. durch einen geheimen Grundschlüssel und einen nicht geheimen , zufälligen Zusatzschlüssel bestimmt sind. Bei jeder Neuinitialisierung des Systems (erste Uebertragungsaufnahme, Wiederaufnahme nach Störung, etc.) wird automatisch ein neuer zufälliger Zusatzschlüssel erzeugt, klar übertragen und sende- und empfangsseitig in die Chiffrier/Dechiffriergeneratoren geladen. Der geheime Grundschlüssel hingegen wird in der Regel nur in relativ grossen Zeitabständen gewechselt.

Bei älteren Systemen erfolgt der Grundschlüsselwechsel durch direkte Eingabe des neuen Schlüssels in den Generator über eine Tastatur oder dgl. Die oben genannten Geräte GC-505 und GC-515 verfügen sende- und empfangsseitig über je einen Speicher, in dem eine Anzahl (z.B. 30) sende- und empfangsseitig identischer geheimer Grundschlüssel vorrätig gehalten wird. Zum Wechseln des Grundschlüssels braucht beim GC-515 nur noch an jeder Station via Wählschalter oder dgl. die Speicheradresse oder Nummer des gewünschten Schlüssels eingegeben zu werden, die Ladung des Schlüssels in den Chiffriergenerator erfolgt dann automatisch. Schlüsseländerungen (z.B. auf die nächsthöhere Schlüsselnummer) werden in bestimmten, zwischen den Partnerstationen vereinbarten Zeitabschnitten vorgenommen. Beim GC-505 genügt es, die Schlüsseladresse in der aufrufenden Station zu wählen, worauf sie automatisch zur Partnerstation übertragen wird.

Bei der chiffrierten Uebertragung muss die für eine eine bestimmte feste Schlüsseleinstellung übertragene Datenmenge (Anzahl Bit) aus Sicherheitsgründen bekanntlich beschränkt werden. Eine obere Grenze ist durch die strukturbedingte Rekursionslänge der zur Verwendung gelangenden Chiffriergeneratoren gegeben. Die maximale Rekursionszeit,während welcher mit unveränderter Schlüsseleinstellung gearbeitet werden darf, hängt von dieser Rekursionslänge ab und ist natürlich umgekehrt proportional der Uebertragungsrate. So wird beispielsweise für das genannte Gerät GC-515 bei einer Uebertragungsrate von 19,2 kb/S eine wöchentliche Aenderung des Grundschlüssels empfohlen. Da der Schlüsselspeicher des GC-515 total 30 Schlüssel enthält, müsste der Speicher bei Dauerbetrieb also alle sechs bis sieben Monate ersetzt werden. Diese relativ häufige Aenderung des Grundschlüssels und der häufige Ersatz der Schlüsselspeicher bedingen einen unerwünschten administrativen und personellen Aufwand, der, dem Trend zu höheren Uebertragungsraten folgend, in Zukunft noch grösser werden dürfte.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Chiffrier/Dechiffriersystem der eingangs definierten Art so zu verbessern, dass seine mit Wahl und Wechsel von Chiffrierschlüsseln zusammenhängende Bedienung möglichst vereinfacht wird bzw. vollständig entfällt.

Diese Aufgabe wird erfindungsgemäss durch die im Patentanspruch 1 angeführten Merkmale und Massnahmen gelöst.

Beim erfindungsgemässen System wird der Grundschlüssel statt durch bewusstes, manuelles Wählen (wie z.B. beim genannten Gerät GC-515) einer Schlüsseladresse oder -nummer durch eine von einem Zufallsgenerator, der vorzugsweise gleich der für die Erzeugung des

Zusatzschlüssels ohnehin vorhandene ist, erzeugte Zufallsadresse ausgewählt. Dabei sind alle Schlüsseladressen gleich wahrscheinlich, sodass über eine längere Zeit eine statistisch relativ gut ausgeglichene Betriebszeit jedes einzelnen Grundschlüssels gewährleistet ist. Durch den häufigen, statistischen Wechsel des Grundschlüssels werden, vor allem bei beschränktem oder sporadischem Betrieb des Systems, die Freiheitsgrade des Schlüsselspeichers kryptologisch besser ausgenutzt. Der automatische Schlüsselwechsel vereinfacht das Schlüsselmanagement und lässt das Chiffriergerät zu einer praktisch unbedienten Black Box werden. Durch den Wegfall der manuellen Schlüsselwahl und der dafür nötigen Bedienungselemente wird das Chiffriergerät schliesslich auch billiger.

Im folgenden wird die Erfindung anhand der Zeichnung näher erläutert. Es zeigen:

Fig. 1 ein Blockschaltbild eines ersten Ausführungsbeispiels,

Fig. 2-4 je eine Skizze zur Erläuterung von dessen Funktionsweise,

Fig. 5 und 6 Blockschaltschemata von zwei weiteren Ausführungsbeispielen und

Fig. 7 eine weitere Skizze zur Funktionserläuterung.

Das in Fig. 1 dargestellte Chiffrier/Dechiffriersystem besteht aus einem gesamthaft mit E bezeichneten Chiffrierteil und einem gesamthaft mit D bezeichneten Dechiffrierteil, die über eine allgemein als Kanal C bezeichnete Datenverbindung in gegenseitiger Verbindung stehen.

Der Chiffrierteil E umfasst im wesentlichen eine u.a. einen Chiffriergenerator 11 und eine Ladekontrolle 12 enthaltende Chiffriereinheit 1, einen Grundschlüsselspeicher 2, einen Zufallsgenerator 3 und eine Auswahlstufe 4. In ähnlicher Weise umfasst der Dechiffrierteil D eine Dechiffriereinheit 5 mit einem Dechiffriergenerator 51 und einer Ladekontrolle 52, einen Grundschlüsselspeicher 6 und eine

Verteilerstufe 7.

Die Auswahlstufe 4 umfasst einen Zähler 41, einen von diesem gesteuerten Schalter 42 und einen Speicher 43 für eine Synchronisiersequenz. Anstelle des Speichers könnte natürlich auch ein entsprechender Generator vorhanden sein, der die Synchronisiersequenz bei Bedarf erzeugt.

Die Verteilerstufe umfasst analog zur Auswahlstufe 4 eine Erkennungsstufe 71 für die Synchronisiersequenz, einen Zähler 72 und einen vom Zähler 72 gesteuerten Schalter 73.

Der Aufbau des in Fig. 1 dargestellten Chiffrier/Dechiffriersystems entspricht bis auf einige Besonderheiten im wesentlichen dem der schon genannten Chiffriersysteme GC 505 und GC 515 der Firma Gretag AG, Regensdorf, Schweiz. Diese Chiffriersysteme werden seit mehreren Jahren weltweit verkauft, sodass ihre Konzeption und ihre Funktionsweise dem Fachmann geläufig sind. Die vorliegende Beschreibung beschränkt sich daher auf das für das Verständnis der Erfindung Wesentliche, wobei alles, was hier nicht speziell erläutert ist, als funktionell ähnlich wie bei den beiden genannten Chiffriersystemen anzunehmen ist.

Die generelle Funktionsweise des dargestellten Systems ist wie folgt:

Zur Aufnahme einer Verbindung wird zunächst über einen im Chiffrierteil E vorhandenen Eingang 9 ein Initialisierungsbefehl gegeben. Durch diesen Befehl wird ein Initialisierungszyklus veranlasst, bei dem Chiffrier- und Dechiffrierteil mittels der Synchronisiersequenz synchronisiert werden, vom Zufallsgenerator 3 ein Zusatzschlüssel AK erzeugt, übertragen und in Chiffrier- und Dechiffriergenerator eingelesen wird, und ferner vom Zufallsgenerator 3 auch

eine zufällige Auswahl-Adresse KA_j für die im Grundschlüsselspeicher 2 gespeicherten Grundschlüssel PK_j erzeugt, die Adresse übertragen und der entsprechende Grundschlüssel PK_j in Chiffrier- und Dechiffriergenerator eingelesen wird.

Dieser Initialisierungszyklus verläuft mit der einzigen, allerdings das Kernstück der Erfindung bildenden Ausnahme, dass die Auswahl des Grundschlüssels nicht von Hand sondern durch den Zufallsgenerator 3 zufallsmässig gesteuert ist, völlig gleich wie bei den schon genannten bekannten Chiffriersystemen GC 505 und GC 515. Schaltungstechnisch findet dies darin seinen Niederschlag, dass der Eingang 44 der Auswahlstufe 4 und der Adresseingang des Speichers 2 nicht mit einer manuellen Eingabevorrichtung, sondern mit dem Zufallsgenerator 3 verbunden sind.

Der Initialisierungszyklus ist in Fig. 2 nochmals veranschaulicht:

Zunächst wird die Synchronisiersequenz SS ausgesandt, dann die Adresse KA_j für den jeweiligen Grundschlüssel PK_j und schliesslich der zufällige Zusatzschlüssel AK. Die beiden letzteren könnten natürlich auch in der Reihenfolge vertauscht sein bzw. könnte die Adresse im Zusatzschlüssel in irgend einer Form enthalten sein. Die Zähler 41 und 72 überwachen (letzterer nach Freigabe durch die Erkennungsstufe 71) die gerade übertragene Information (Synchronisiersequenz, Schlüsseladresse etc.) und veranlassen bei Erreichen der jeweils vorgegebenen Längen (Bitzahlen) dieser Informationen eine Umschaltung der Schalter 42 und 73 in die dem richtigen Datenfluss entsprechenden Schaltstellungen sowie im Dechiffrierteil über die Ladekontrolle 52 auch das Laden der Schlüssel PK und AK in den Dechiffriergenerator 51.

Nach Abschluss des Initialisierungszyklusses sind Chiffrier- und Dechiffriergenerator synchronisiert und mit jeweils dem gleichen

Grund- und Zusatzschlüssel PK_j bzw. AK geladen. Die Schalter 42 und 73 befinden sich wieder in ihrer gezeigten Ausgangsstellung. Nunmehr können der Chiffriereinheit 1 Klardaten CD zugeführt und von dieser in bekannter Weise chiffriert werden. Das dabei entstehende Chiffrat CT gelangt dann über die Auswahlstufe 4, den Kanal C und die Verteilerstufe 7 in die Dechiffriereinheit 5 und wird dort wieder in den ursprünglichen Klartext CD zurückverwandelt.

Der zur Verwendung gelangende Grundschlüssel PK_j wird also bei jeder Neuinitialisierung durch den Zufallsgenerator 3 zufallsmässig ausgewählt. Der Zufallsgenerator kann für die Adressinformation einen einzigen Ausgang besitzen, es ist aber auch ohne weiteres denkbar, die Adressinformation direkt aus dem ohnehin vorhandenen, ebenfalls zufälligen Zusatzschlüssel abzuleiten, z.B. etwa über eine Polynom-Verknüpfung.

Die Adresse des z.B. durch die aufrufende Station zufällig ausgewählten Grundschlüssels wird klar zum Empfänger übertragen, wobei vorzugsweise fehlerkorrigierende oder fehlererkennende Codes verwendet werden.

Durch die zufallsmässige Auswahl der Grundschlüssel aus dem gespeicherten Vorrat ist jede Adresse gleich wahrscheinlich. Eine "Buchführung" zur Vermeidung mehrmaligen Aufrufen desselben Schlüssels ist daher nicht unbedingt nötig.

In einem praktischen Beispiel können die Schlüsselspeicher z.B. 256 verschiedene Schlüssel à je 64 Bit aufnehmen. Ein derartiger Speicher lässt sich derzeit ohne weiteres in einer einzigen integrierten Schaltung (PROM) realisieren. Bei fünfjährigem Betrieb des Systems würde im Duchschnitt jeder Schlüssel eine Woche lang verwendet. Bei Neuinitialisierungen in Intervallen von durchschnittlich 5 - 6 Stunden würde dann jeder Schlüssel während der

fünfjährigen Betriebszeit im Durchnitt etwa 32 mal benutzt, was für einen relativ guten statistischen Ausgleich der Betriebszeiten der einzelnen Schlüssel sorgen sollte.

Eine Neuinitialisierung des Systems und damit ein Wechsel des Grundschlüssels (und gegebenenfalls auch des Zusatzschlüssels) wird generell bei Netzunterbruch, Leitungsunterbruch, Aktivierung eines Selbsttestes, Verlust des Byte-Taktes und Wechsel der Uebertragungsrichtung vorgenommen. Ein neuer Grundschlüssel kann ferner auch verwendet werden, wenn eine vorgegebene maximale Datenmenge N_{max} verarbeitet ist. Letztere beträgt zweckmässig nur einen Bruchteil der Rekursionslänge des Chiffriergenerators und ist ferner klein genug, um während der vorgesehenen Betriebszeit des Schlüsselspeichers eine statistisch ausgeglichene Durchmischung aller Schlüssel erwarten zu lassen.

Die zu einer Neuinitialisierung führende Ereignisse sind in Fig. 3 nochmals schematisch zusammengefasst. Die Kästchen 92 - 96 symbolisieren Sensoren bzw. Detektoren für die betreffenden Ereignisse, wobei die Kästchen 93 und 95 stellvertretend für alle möglichen Störungen dastehen. Die Ausgänge der Ereignissensoren sind in einem Oder-Tor 91 zusammengefasst, das seinerseits mit dem Initialisierungseingang 9 des Chiffrierteils 1 verbunden ist, sodass also bei Ansprechen irgendeines der Sensoren eine Initialisierung ausgelöst wird.

Es versteht sich, dass die Darstellung nach Fig. 3 rein symbolhaft ist und in Realität selbstverständlich auch anders gelöst sein kann.

Ueberhaupt ist das ganze Chiffriersystem mit Vorteil in Form eines Mikrocomputersystems realisiert, bei welchem die einzelnen Operationen und Datenflüsse programmgesteuert ablaufen.

Aus Geschwindigkeits- oder anderen Gründen können dabei einzelne Komponenten, wie z.B. Teile des Chiffriergenerators etc, natürlich auch in Hardware implementiert sein. Die vorliegende Beschreibung und die Figuren sollen lediglich die für die Erfindung wesentlichen Funktionsgruppen erklären, wobei es keine Rolle spielt, ob diese Gruppen durch spezifische Hardware oder in einem Mikrocomputersystem softwaremässig implementiert sind. Als Beispiel für ein mit einem Mikrocomputersystem ausgerüstetes Chiffriersystem sei hier nur das schon genannte Gerät GC-505 angeführt.

Anstatt den Grundschlüssel PK jeweils nur bei einer Neuinitialisierung zu wechseln, kann der Schlüsselwechsel auch gemäss dem folgenden, in der Fig. 4 an einem Beispiel verdeutlichten Prinzip vorgenommen werden:

Bei Beginn der Uebertragung erfolgt eine Neuinitialisierung, wobei ein erster zufälliger Zusatzschlüssel AK 1 und ein erster, zufällig ausgewählter Grundschlüssel erzeugt bzw. aus dem Speicher 2 ausgelesen werden. In Fig. 4 ist angenommen, im Speicher befindet sich ein Vorrat von acht Grundschlüsseln, die von 0 - 7 durchnummeriert sind. Der erste ausgewählte Grundschlüssel ist hier durch die Nummer 3 markiert. Mit dieser Schlüsseleinstellung AK 1 - PK 3 wird nun chiffriert bzw. dechiffriert. Nach Verarbeitung einer vorgegebenen maximalen Datenmenge N_{max}, die natürlich von der Rekursionslänge des Chiffriergenerators abhängt, wird bei gleichbleibendem Zusatzschlüssel AK 1 ein neuer Grundschlüssel ausgewählt und eingestellt. Der Einfachheit halber ist dies in der Regel gleich der Schlüssel mit der nächstfolgenden Speicheradresse, im Beispiel hier also der Grundschlüssel No. 4. Mit dieser neuen Schlüsselkombination AK 1 - PK 4 wird nun wieder - störungsfreier Betrieb vorausgesetzt - solange gearbeitet, bis die maximale Datenmenge N_{max} verarbeitet ist. Daraufhin wird der nächstfolgende Grundschlüssel eingestellt und so weiter, bis alle Schlüssel (hier acht) im Speicher

einmal benützt worden sind. Danach erfolgt automatisch eine neue Initialisierung unter Erzeugung eines neuen zufälligen Zusatzschlüssels AK 2 und einer neuen Anfangsadresse - hier z.B. No. 7 - für die Grundschlüssel PK..

Nach diesem Schema wird solange fortgefahren, bis irgendein Ereignis eintritt,welches eine Neuinitialisierung erzwingt. In Fig. 4 sind diese Ereignisse durch das Symbol ⊗ bezeichnet. Nach erfolgter Neuinitialisierung wird dann wieder im beschriebenen Rhythmus weiter gearbeitet, was aus Fig. 4 unschwer erkennbar ist.

Das eben beschriebene Verfahren hat den Vorteil, dass nach Ablauf der maximal vorgegebenen Datenmenge N_{max} ein Schlüsselwechsel ohne Unterbruch der Datenübertragung vorgenommen werden kann, da hier durch die einfache Inkrementierung der Speicheradressen die Schlüsseladressen nicht übertragen werden müssen.

Die Länge N_{max} der maximalen Datenmenge muss selbstverständlich nicht unbedingt konstant sein. Beispielsweise könnte der (Grund-) Schlüsselwechsel auch datenpaketorientiert erfolgen. Eine weitere Möglichkeit wäre, den Schlüsselwechsel, d.h. die Inkrementierung der Grundschlüsseladressen in geheimen, ev. pseudozufällig determinierten Zeitabständen vorzunehmen.

Die zur praktischen Dürchführung des eben beschriebenen Schlüsselwechselschemas notwendigen schaltungstechnischen Massnahmen sind aus Fig. 5 zu ersehen,wobei nur die für das Verständnis dieses Schemas nötigen Teile dargestellt sind und der Rest gleich wie in Fig. 1 ist. Ausserdem sind natürlich auch bei diesem Ausführungsbeispiel des erfindungsgemässen Chiffriersystems die einzelnen Funktionsgruppen vorzugsweise durch ein Mikrocomputersystem realisiert.

Zusätzlich zu den schon in Fig. 1 dargestellten Elementen sind in Fig. 5 sendeseitig noch ein Adresszähler 21 für den Speicher 2, ein Zähler 22 für die Erfassung der verarbeiteten Daten sowie ein Schlüsselzähler 23 und empfangsseitig ein Adresszähler 61 und ein Datenzähler 62 vorhanden.

Bei einer Neuinitialisierung werden alle Zähler zurückgesetzt und die erste Zufallsadresse KA für den Grundschlüssel in den Adresszähler 21 geladen und dann die Verarbeitung der Daten begonnen. Sobald der Datenzähler 22 den vorgegebenen Stand N_{max} erreicht, werden der Adresszähler 21 und der Schlüsselzähler 23 inkrementiert und ein neuer Grundschlüssel in den Chiffriergenerator eingelesen. Dasselbe geschieht sinngemäss natürlich auch im Dechiffrierteil. Wenn der Schlüsselzähler 23 den der im Speicher 2 vorhandenen Anzahl Grundschlüssel PK entsprechenden Stand NK erreicht, veranlasst er über das Oder-Tor 91 und den Eingang 9 einen neuen Initialisierungszyklus und so fort.

Das bisher beschriebene Schlüsselwechselprinzip lässt sich im Sinne einer besseren Speicherausnützung noch etwas verallgemeinern. Statt die gegebene Speicherkapazität N x M der Grundschlüsselspeicher in N unabhängige Schlüssel à je M Bit zu unterteilen, kann eine wesentlich grössere Schlüsselmenge im Speicher untergebracht werden, wenn jeder Schlüssel aus einer spezifizierten Anordnung von M der total M x N Informationselemente besteht. Im extremsten Fall, wo jedes der M Schlüsselbit pro Schlüssel durch eine Zufallsadresse bestimmt würde, wären $(M \times N)^M$ verschiedene Schlüsselkombinationen möglich, wobei davon natürlich nur 2^M gegenseitig unterscheidbar wären. Derart ausgewählte Grundschlüssel würden praktisch idealen Zufallscharakter besitzen, die statistische Ausnützung der Geheimelemente wäre aber nur unzulänglich und die zu übertragende Adressinformation wäre für die Praxis zu lang.

Eine praktisch attraktivere Lösung ist das Abzählen von M Schlüsselbits ab einem zufällig aus der Gesamtheit der M x N Bit ausgewählten Bit. Damit ergeben sich statt N nun M x N Schlüssel, wobei allerdings zu jedem Schlüssel PK_j weitere Schlüsselpaare $PK_{j-\mu}$ und $PK_{j+\mu}$ existieren, welche PK_j um $M-\mu$ Bit überlappen ($1 \leq \mu \leq M-1$). Nicht alle M x N Schlüssel sind unbedingt verschieden, aber sie sind es mit sehr hoher Wahrscheinlichkeit, selbst wenn der Speicherinhalt keinen speziellen Einschränkungen unterworfen ist.

In Fig. 7 ist die eben skizzierte Schlüsselorganisation im Speicher 2 bzw. 6 für N = 2 und M = 4 bildhaft dargestellt. Wie man erkennt, sind acht verschiedene Schlüssel mit den Anfangsadressen 0 - 7 möglich, wobei sich benachbarte Schlüssel jeweils um 3 Bit gegenseitig überlappen.

Die gegenseitige Ueberlappung der Grundschlüssel PK kann, sofern überhaupt erwünscht, klein gehalten werden. Sie kann zum Beispiel dadurch erreicht werden, das man kürzere Startadressen wählt, welche Gruppen von Bits anstelle von Einzelbits definieren. Als Beispiel kann man sich die in Fig. 7 gezeigte Anordnung als Bytes anstelle von Bits vorstellen. Eine Byte-Adressierung als kleinste Einheit ist auch bei den meisten Mikrocomputersystemen software- und hardwaremässig besonders günstig.

Mit einem Festwertspeicher (PROM) von 2048 x 8 Bit Speicherkapazität ergeben sich bei einer Schlüssellänge von M = 64 Bit beispielsweise folgende Möglichkeiten:

Ueberlappung (Bit)	Anzahl Schlüssel	Adressumfang (Bit)
0	256	8
32	512	9
48	1024	10
56	2048	11

In Fig. 6 ist ein Ausführungsbeispiel eines Chiffriersystems dargestellt, welches für die eben beschriebene Schlüsselorganisation mit überlappenden Schlüsseln eingerichtet ist. Es unterscheidet sich gegenüber der Ausführungsform nach Fig. 5 lediglich durch je einen weiteren Adresszähler 24 bzw. 64 und einen Impulsgenerator 25 bzw. 65. Ferner ist noch je ein Transcoder 26 bzw. 66 vorgesehen, die allerdings mit der Schlüsselorganisation an sich nichts zu tun haben und im folgenden zunächst als nicht existent betrachtet werden.

Die Grundschlüsselspeicher 2 und 6 sind hier beispielsweise vom Format 2048 x 8 bit, benötigen also zur Adressierung jeweils eines Bytes eine 11-Bit-Adresse. Jeder Grundschlüssel möge 64 Bit umfassen.

Bei einer Initialisierung wird nun zunächst eine vom Zufallsgenerator 3 gebildete 8-Bit-Adresse in die zweiten Adresszähler 24 bzw. 64 eingelesen. Gleichzeitig werden die acht höherwertigen Bits der ersten, je elf Bit umfassenden Adresszähler 21 bzw. 61 mit dieser Adressinformation geladen. Nunmehr erzeugen die Impulsgeneratoren 25 bzw. 65 eine Sequenz von acht Taktimpulsen, welche die ersten Adresszähler acht mal inkrementieren. Dadurch werden hintereinander acht aufeinanderfolgende Bytes in den Schlüsselspeichern adressiert, wobei nach jedem Schritt das betreffende Byte in den Chiffriergenerator bzw. Dechiffriergenerator eingelesen wird. Nach acht Schritten ergibt dies also eine Gesamtschlüssellänge von 8 Byte entsprechend 64 bit.

Mit dem so eingestellten Grundschlüssel (und Zusatzschlüssel) wird nun entsprechend der Ausführung nach Fig. 5 solange chiffriert, bis die Datenzähler 22 bzw. 62 das Erreichen der vorgegebenen Maximaldatenmenge N_{max} signalisieren. Dann werden zunächst die zweiten Adresszähler 24 bzw. 64 inkrementiert und dann durch achtfaches Inkrementieren der ersten Zähler und jeweils anschliessendes Auslesen der Speicher die 64 Bit des nächstfolgenden Grundschlüssels eingestellt,

u.s.f. Im Übrigen arbeitet dieses Ausführungsbeispiel analog wie das gemäss Fig. 5.

Wie beim Ausführungsbeispiel gemäss Fig. 5 gilt auch hier, dass die diversen Zähler, Impulsgeneratoren etc. vorzugsweise durch ein Mikrocomputersystem realisiert sind.

Wie aus der generellen Funktionsbeschreibung im Zusammenhang mit Fig. 1 hervorgeht, wird die Adresse des Grundschlüssels klar übertragen. Bei den Ausführungsbeispielen nach den Fig. 5 und 6 ist dies natürlich jeweils nur die Startadresse, von der bei jeder Neuinitialisierung ausgegangen wird. Um zu verhindern, dass ein Unbefugter aus der klaren Startadresse und der Ueberlappung der Schlüssel Nutzen zieht (wenn z.B. schon gewisse Schlüssel oder Teile davon bekannt sind), sind den zweiten Adresszählern 24 bzw 64 die schon genannten Transcoder 26 bzw. 66 vorgeschaltet. Diese transformieren die vom Zufallsgenerator 3 gebildete Startadresse nach irgendeiner Gesetzmässigkeit und verschleiern damit das Ueberlappungsgesetz.

Patentansprüche

1. Chiffrier/Dechiffriersystem mit einem Chiffrierteil (E) mit Mitteln (1) zum Umwandeln von Klardaten (CD) in ein Chiffrat (CT) und einem Dechiffrierteil (D) mit Mitteln (5) zum Rückumwandeln des Chiffrats (CT) in Klardaten (CD), wobei der Chiffrierteil (E) einen Chiffriergenerator (11), dessen Anfangszustand und/oder Struktur wenigstens durch einen ersten geheimen Schlüssel (PK) bestimmt wird, sowie einen ersten Speicher (2) mit einer Anzahl verschiedener erster Schlüssel (PK) enthält, und wobei der Dechiffrierteil (D) einen gleich wie der Chiffriergenerator (11) aufgebauten Dechiffriergenerator (51) sowie einen zweiten Speicher (6) mit denselben ersten Schlüsseln (PK) wie im ersten Speicher (2) enthält, und wobei Chiffrier- und Dechiffrierteil ferner Schlüsselladeмittel (12,4,7,52) enthalten, um bei einer Neuinitialisierung des Systems einen ersten Schlüssel (PK) aus dem ersten Speicher (2) auszuwählen, in den Chiffriergenerator (11) zu laden, die Speicher-Adresse (KA) des ausgewählten ersten Schlüssels (PK) zum Dechiffrierteil (D) zu übertragen und dort aufgrund der übertragenen Speicheradresse (KA) denselben ersten Schlüssel (PK) aus dem zweiten Speicher (6) auszulesen und in den Dechiffriergenerator (51) zu laden, dadurch gekennzeichnet, dass die Schlüsselladeмittel (12,4,7,52) durch eine im Chiffrierteil (E) befindliche Zufallsstufe (3) gesteuert sind, welche bei jeder Neuinitialisierung des Systems eine zufällige Auswahladresse (KA) für die im ersten und zweiten Speicher (2,6) enthaltenen und bei der Neuinitialisierung neu zu ladenden ersten Schlüssel (PK) bildet.

2. System nach Anspruch 1, wobei Chiffrier- und Dechiffriergenerator (11,51) je durch die genannten ersten und durch zweite, zufällige Schlüssel (AK) determiniert sind, wobei der Chiffrierteil (E) einen Zufallsgenerator (3) zur Erzeugung dieser zweiten Schlüssel (AK) enthält und wobei ferner die genannten Schlüsselladeмittel (12,4,7,52) in Chiffrier- und Dechiffrierteil dazu ausgebildet sind,

bei jeder Neuinitialisierung des Systems einen zweiten Schlüssel (AK) in den Chiffriergenerator (11) zu laden, zum Dechiffrierteil (D) zu übertragen und dort in den Dechiffriergenerator (51) zu laden, dadurch gekennzeichnet, dass die genannte Zufallsstufe durch den Zufallsgenerator (3) gebildet ist.

3. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass im Chiffrier- und Dechiffrierteil je Inkrementiermittel (21, 22, 23; 61, 62) vorhanden sind, welcher nach Uebertragung von je einer vorgegebenen Datenmenge (N_{max}) automatisch in Chiffrier- und Dechiffrierteil das systematische Auslesen und Laden jeweils eines neuen ersten Schlüssels (PK) aus dem ersten bzw. zweiten Speicher (2,6) in den Chiffrier- bzw. Dechiffriergenerator (11,51) ohne Uebertragung der betreffenden Speicheradresse (KA) bewirken, und welche ferner nach dem Auslesen wenigstens eines Teils der gespeicherten ersten Schlüssel (PK) eine Neuinitialisierung des Systems veranlassen.

4. System nach einem der Ansprüche 1 - 3, dadurch gekennzeichnet, dass Chiffrier- und Dechiffrierteil Mittel (91-96) enthalten, welche auf Uebertragungsaufnahme und/oder Uebertragungsstörungen und/oder Richtungswechsel der Uebertragung und/oder Verarbeitung einer vorgegebenen maximalen Datenmenge ansprechen und bei bzw. nach diesen Ereignissen eine Neuinitialisierung des Systems bewirken.

5. Vorrichtung nach einem der Ansprüche 1 - 4, dadurch gekennzeichnet, dass der Chiffrierteil (E) eine Transformationsstufe (26) zum Kodieren der von der Zufallsstufe (3) erzeugten Speicheradressen (KA) der ersten Schlüssel (PK) und der Dechiffrierteil (D) eine entsprechende Rücktransformationsstufe (66) zur Dekodierung der Speicheradressen (KA) aufweist.

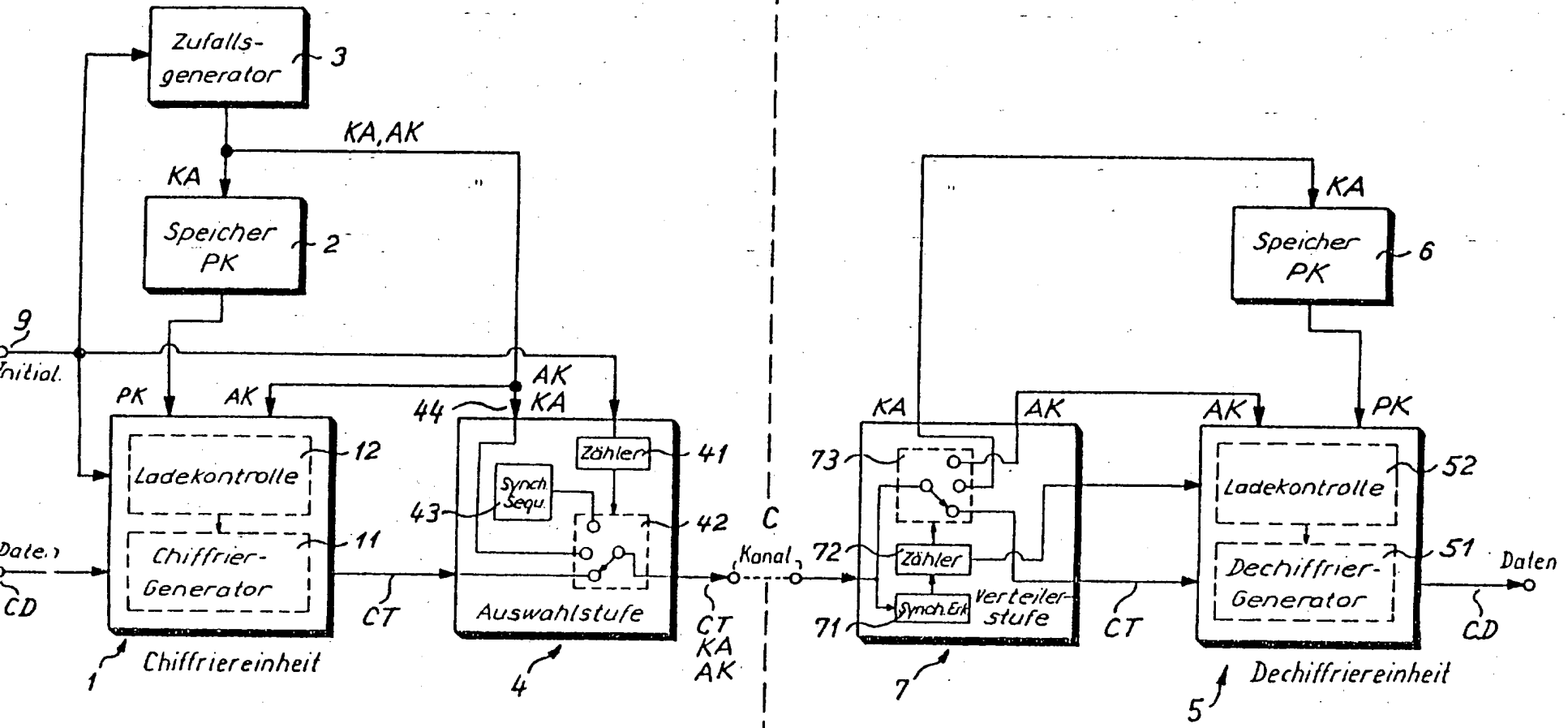

Zufalls-
generator
3
KA,AK
KA
Speicher
PK
2
9
Initial.
PK
AK
AK
KA
44
12
Ladekontrolle
11
Chiffrier-
Generator
Date.
CD
CT
Zähler
41
Synch
Sequ.
43
42
Auswahlstufe
CT
KA
AK
1
Chiffriereinheit
4
C
Kanal
KA
AK
Speicher
PK
6
73
72
71
Zähler
Synch.Erk
Verteiler-
stufe
CT
7
AK
PK
Ladekontrolle
52
Dechiffrier-
Generator
51
Daten
CD
5
Dechiffriereinheit
Chiffrierteil E
Dechiffrierteil D

Fig. 1

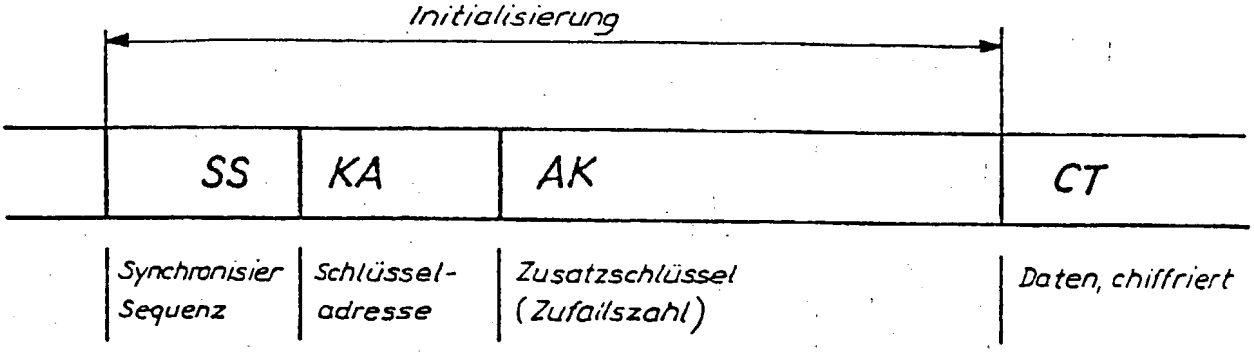

Initialisierung
SS
KA
AK
CT
Synchronisier Sequenz
Schlüssel-adresse
Zusatzschlüssel (Zufallszahl)
Daten, chiffriert

Fig. 2

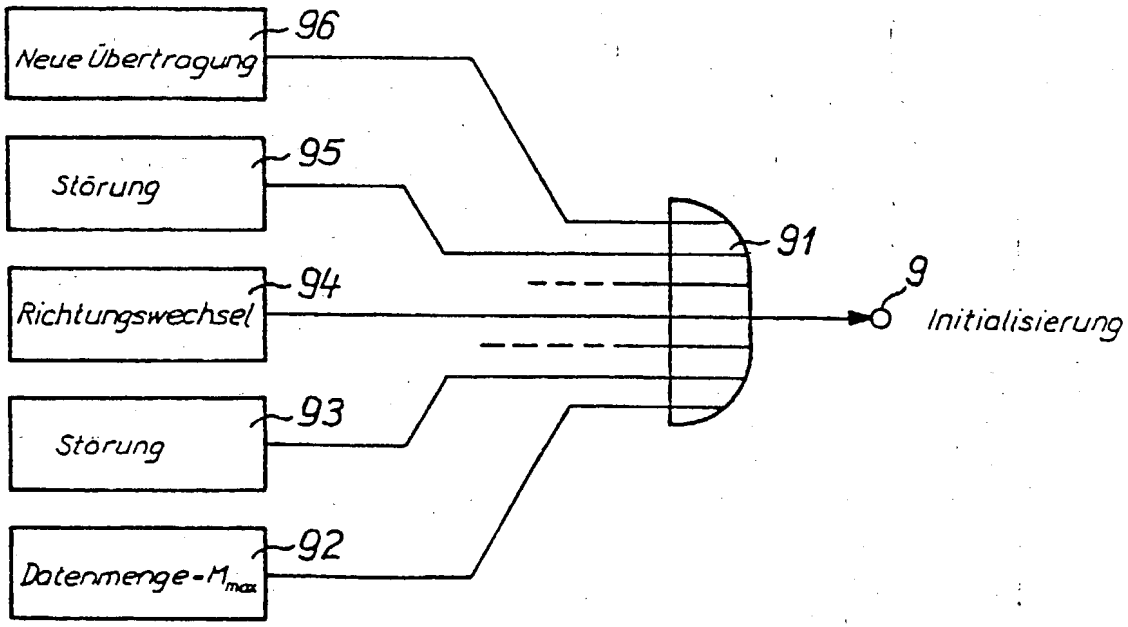

Neue Übertragung
96
Störung
95
Richtungswechsel
94
Störung
93
Datenmenge-M_{max}
92
91
9
Initialisierung

Fig. 3

AK \ PK	Grundschlüsselnummer (-adresse) PK · (KA)								
1	3	4	5	6	7	0	1	2	störungsfreier Betrieb
2	7	0	1	2	3	4	5	6	
3	4	5	⊗						
4	1	2	3	4	5	6	7	0	störungsfrei
5	2	3	4	5	⊗				
6	6	7	0	1	2	3	4	5	störungsfrei
7	5	6	7	0	.....				
⋮									

Fig. 4

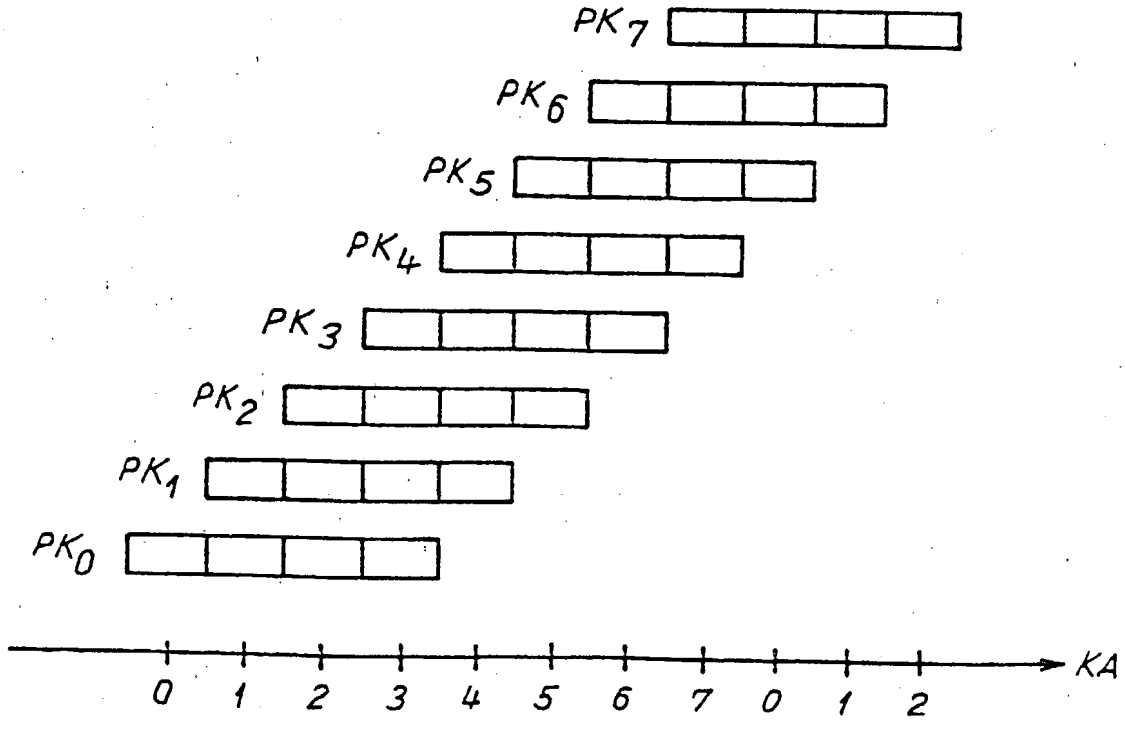
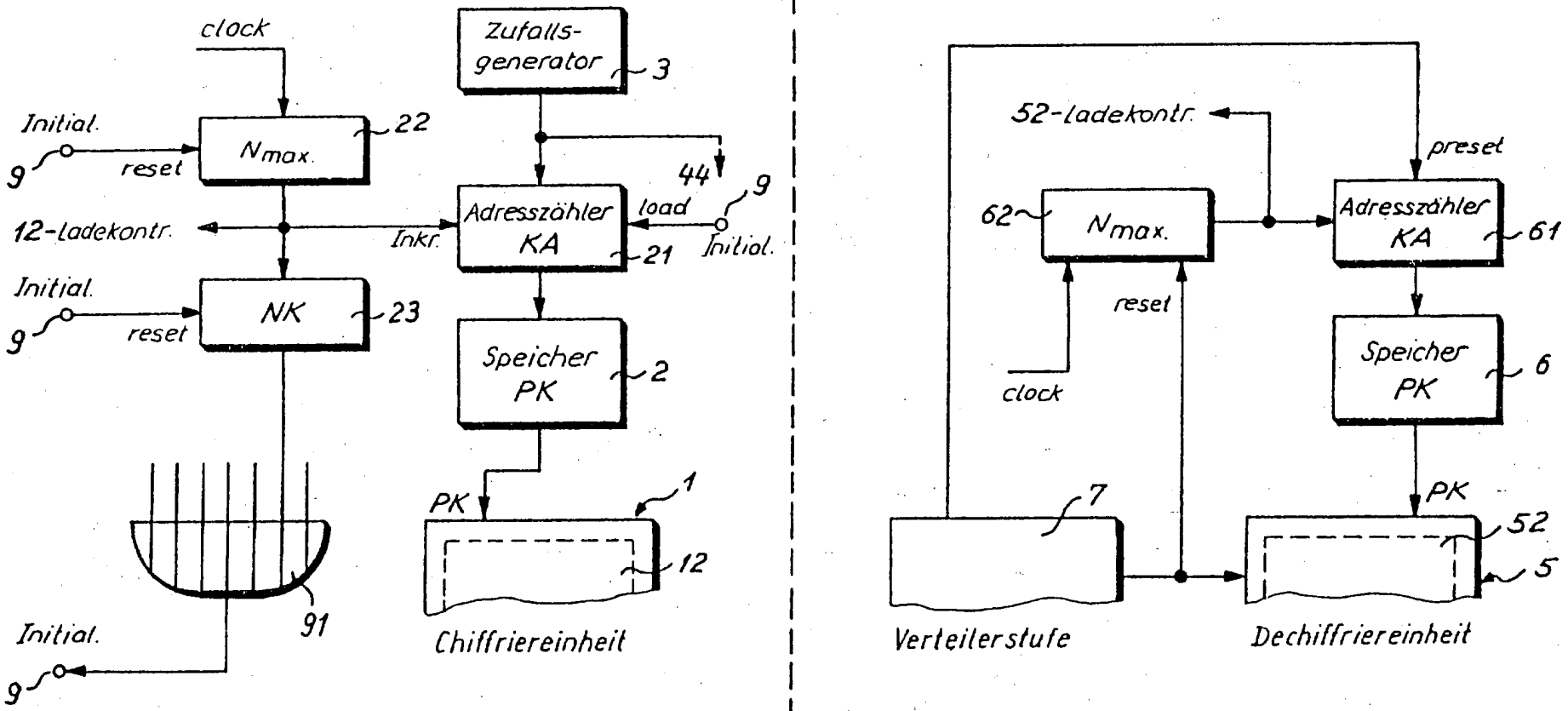


Fig. 7



Chiffrierteil E

Dechiffrierteil D

Fig. 5

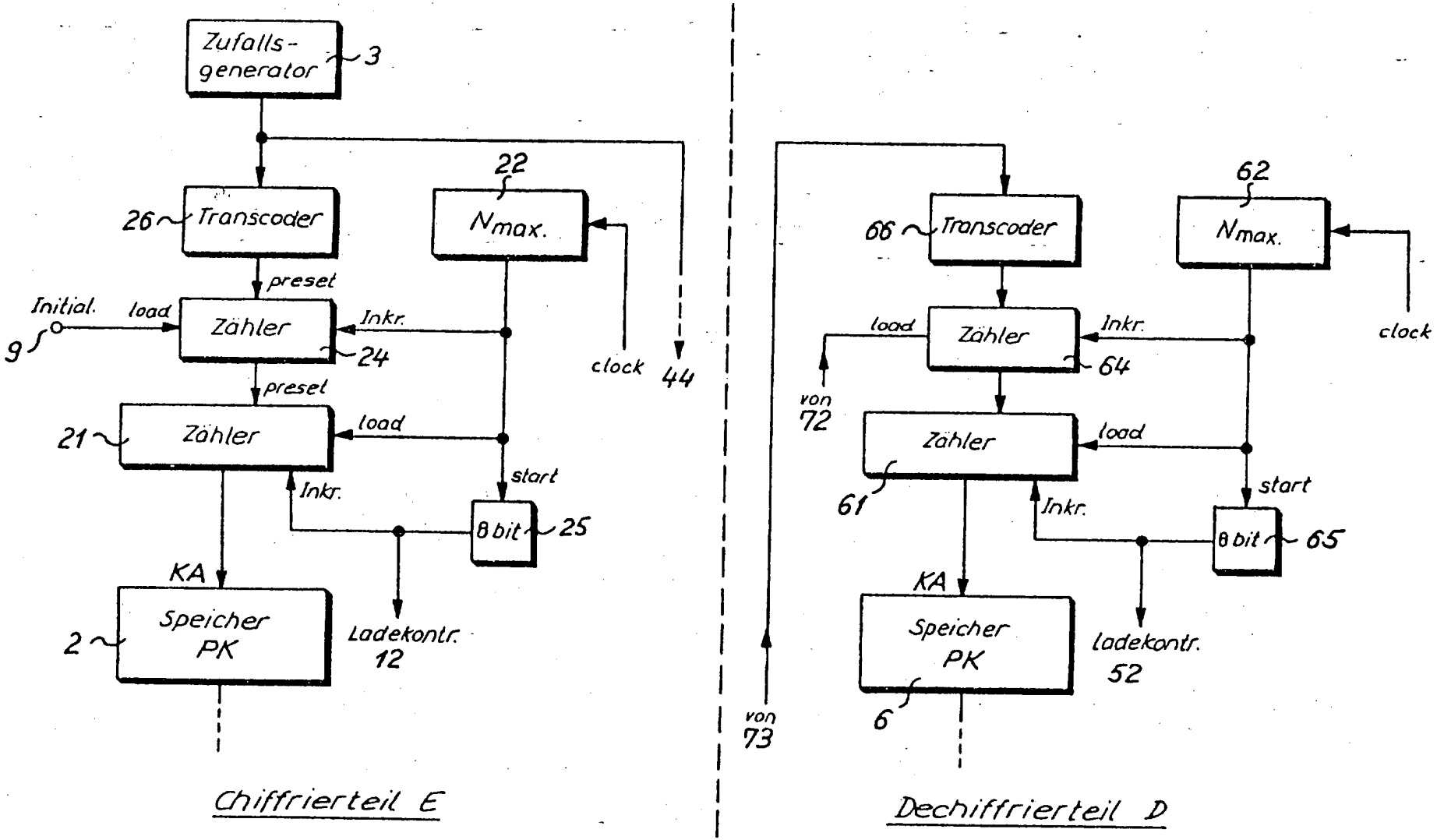

Zufalls-generator
3
22
Nmax.
26
Transcoder
preset
Initial.
load
Zähler
Inkr.
9
24
clock
44
preset
21
Zähler
load
start
Inkr.
8 bit
25
KA
Speicher PK
2
Ladekontr.
12
Chiffrierteil E
62
Nmax.
66
Transcoder
load
Zähler
Inkr.
clock
64
von
72
Zähler
load
start
61
Inkr.
8 bit
65
KA
Speicher PK
Ladekontr.
52
6
von
73
Dechiffrierteil D

Fig. 6

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 80 81 0391

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	betrifft Anspruch
	FR - A - 2 210 307 (IBM) * Seite 2, erster Abschnitt; Seite 4, Zeilen 2-11, 19-36; Seite 5, Zeilen 8-15, 23-38. *	1
	FR - A - 2 288 428 (ERICSSON) * Seite 2, Zeilen 1-17; Seite 3, Zeile 16 bis Seite 4, Zeile 17; Seite 5, Zeile 34 bis Seite 6, Zeile 7, Zeilen 14-17 *	1,5
	ELECTRONICS, Band 52, Heft 13, 21. Juni 1979, NEW YORK (US) HINDIN: "LSI-bsed data encryption discourages the data thief", Seiten 107-120 * Seite 115, linke Spalte, Zeile 31 bis rechte Spalte, Zeile 6 *	1
A	DE - A - 2 334 330 (LICENTIA) * Seite 3, Zeile 1 bis letzte Zeile; Seite 8, Zeilen 1-4, Zeile 11 bis letzte Zeile; Seite 9, letzter Absatz bis Seite 10, Zeile 16 *	1
A	US - A - 3 291 908 (EHRAT) * Spalte 2, Zeilen 37-51 *	2

KLASSIFIKATION DER ANMELDUNG (Int. Cl.)

H 04 L 9/00

RECHERCHIERTE SACHGEBIETE (Int. Cl.)

H 04 L 9/02
9/00
9/04

KATEGORIE DER GENANNTEN DOKUMENTE

X: von besonderer Bedeutung
A: technologischer Hintergrund
O: nichtschriftliche Offenbarung
P: Zwischenliteratur
T: der Erfindung zugrunde liegende Theorien oder Grundsätze
E: kollidierende Anmeldung
D: in der Anmeldung angeführtes Dokument
L: aus andern Gründen angeführtes Dokument
&: Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt.

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	30.03.1981	HOLPER